

DOCKET FILE COPY ORIGINAL

ORIGINAL

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

RECEIVED

DEC - 6 2002

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Digital Broadcast Copy Protection

)
)
)
)
)

MB Docket No. 02-230

COMMENTS OF MOTOROLA

Jeanine Poltronieri
Director, Telecommunications Strategy
and Regulation
Eric J. Sprunk
Senior Director, Advanced Technology
Broadband Communications Sector

Motorola
1350 I Street, N.W.
Washington, DC 20005-3305
Tel: 202-371-6870

December 6, 2002

No. of Copies rec'd 04
List ABCDE

TABLE OF CONTENTS

	Page
SUMMARY	ii
I. Motorola Has A Wide Range Of Interests At Stake In DTV Transition And Wants To Enable A Speedy Transition	1
II. Realistic Acknowledgement Of Security Challenges Is Necessary To Ensure Appropriate Level Of Investment In Digital Broadcast Copy Protection Solutions And To Facilitate The Transition To DTV	3
III. Any Comprehensive DTV Digital Broadcast Copy Protection Solution Must Encrypt At The Source.	4
IV. Deployment Of Source Encryption For DTV Need Not Disenfranchise Early Adopter Consumers.....	6
V. Source Encryption Equipment Upgrades Are Optional, Not Mandatory, And Can Be Financed Through Normal Competitive Market Forces	8
VI. Source Encryption Is Not Synonymous With Pay TV, And Can Be Applied To Free TV Where Needed For Copy Protection Security	9
VII. Any Mandated Source-Encrypting Digital Broadcast Copy Protection Solution Must Provide For A Minimal Licensing Or Cost Burden	9
VIII Any Mandated Digital Broadcast Copy Protection Solution Must Be Administered By A Transparent Process Governed By An Open Governing Body	10
CONCLUSION	12

SUMMARY

Motorola's position as a major consumer electronics manufacturer, designing everything from cable modems and set-top equipment to wireless handsets, provides it with a unique perspective on developing DTV technology. As explained in more detail in the accompanying comments, although there is reason to question the achievability of a market-based broadcast copy protection solution, Motorola believes that such a solution should be vigorously pursued prior to any regulatory action.

Motorola believes that the broadcast flag, as defined today without source encryption, is an ineffective security technology that ultimately will not serve the interests of the DTV transition or the consumer community. The use of source encryption is so well-established and commonplace that networks which traffic in valuable content without source encryption are the exception, not the rule.

It is not necessary that currently-deployed DTVs be replaced or even augmented to facilitate broadcast copy protection that utilizes source encryption. Some advertising revenue-based services seek the widest audience possible and *are* not concerned about the need to source encrypt, for example.

Source encryption would only be activated for premium and long-lived content. The early adopter population would always have access to the unencrypted "copy freely" grade of content, but would not be able to receive the encrypted higher grades without obtaining new, source decryption-enabled devices. To offer upgrade equipment to consumers who so desire, various technical solutions will be designed to support early adopter DTVs that have been deployed without source decryption technology, as well as the existing analog TV base. Families of devices will be developed that would act as

bridge products to address analog televisions and the DTVs that have already been deployed without the encryption technology.

In order for any source-encryption DTV solution to be deployed widely, any licensing burden must be low to facilitate the most rapid and widest possible usage in DTVs and DTV compatible devices. To maximize viability, any contract to use this technology must be free from burdensome licensing terms that prevent the solution from being freely available and universally deployed. As is common in today's leading edge technology standards, such broadcast copy protection technology must be made openly available to all interested parties under fair, reasonable, and non-discriminatory terms.

The technology for source encryption of DTV must be developed through a standards-based process, be it an existing body or one that follows typical standards **rules** and processes and is convened exclusively for DTV broadcast copy protection. Such a technology standard must be completely open, without closed-door meetings or private decision making processes.

However, a separate governing body should be established to handle various broadcast copy protection implementation, deployment, and usage issues including licensing the numerous manufacturers who will need the technology for DTVs and related products. The governing body must have a balanced membership that includes representatives from all stakeholders. The governing body must be managed by a transparent process that is auditable and open.

While such a body may not necessarily be convened by the FCC as a Federal Advisory Committee formally, and may exist as an industry and market led initiative, the rules established in the Federal Advisory Committee Act may serve as a model.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Digital Broadcast Copy Protection)	MB Docket No. 02-230
)	
)	

COMMENTS OF MOTOROLA

Motorola hereby submits these comments in response to the FCC's Notice of Proposed Rule Making in the above-captioned proceeding.¹ Motorola takes this opportunity to comment on the need for any digital broadcast copy protection to include encryption at the source if it is to be effective.

1. Motorola has a Wide Range of Interests at Stake in DTV Transition and Wants to Enable a Speedy Transition.

Motorola's position as a major consumer electronics manufacturer, designing everything from cable modems and set-top equipment to wireless handsets, provides it with a unique perspective on developing DTV technology. The transition to DTV in the United States affects almost every business sector within Motorola. Motorola is a leading manufacturer of digital consumer and commercial terminals designed to deliver broadband communications, including DTV, to multichannel video subscribers, over its advanced end-to-end digital cable, satellite, and terrestrial broadcast system equipment. Motorola also produces the advanced infrastructure and customer handset equipment for those wireless communications that will utilize spectrum in the 698-806 MHz bands once it is vacated by broadcasters as a result of the DTV transition

¹ *In the Matter of Review of Digital Broadcast Copy Protection*, MB Docket No. 02-230, FCC 02-231, Notice of Proposed Rule Making, released August 9, 2002.

Motorola has participated in numerous Commission proceedings related to the DTV transition, commenting extensively on the technical characteristics of the spectrum at issue in the Commission proceeding regarding service and operational rules', as well as the need to promote a speedy transition to DTV in order to make the spectrum available to wireless communications entities, including public safety users, private wireless carriers and commercial wireless carriers.³ Motorola has pointed out that the public interest benefits of a speedy transition are twofold: to provide consumers with the benefits of vibrant digital video services and to ensure that public safety organizations, including first responders, have access to the spectrum currently used for analog broadcast television.⁴

As always, the Commission must be cautious regarding any activity that may alter the development of market forces, and the presumption should be against regulation unless a compelling showing is made that government action is necessary to ensure a consumer benefit and advance the public interest. However, as Commissioner Abernathy has pointed out: "[t]he transition to digital has never been a marketplace transition, but one mandated by Congress." This government-mandated transition is further complicated by the fact that a number of different steps need to be taken in parallel. Chairman Powell has stated: "[u]ltimately, the DTV transition will shift into high gear when three factors come

² See, e.g., *In the Matter of Service Rules for the 746-764 and 776-794 MHz Bands and Revision to Part 27 of the Commission's Rules*, WT Docket 99-168.

³ See, e.g., *In the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communication Requirements Through the Year 2010, Establishment of Rules and Requirements for Priority Access Service*, WT Docket No. 96-86.

⁴ See Motorola Press Statement Regarding Draft Legislation prepared by House Commerce Committee Chairman Bill Tauzin and Ranking Member John Dingell, September 24, 2001.

⁵ Separate Statement of Commissioner Kathleen Q. Abernathy, *In the Matter of Review of the Commissioner's Rules and Policies Affecting the Conversion to Digital Television*, MM Docket No. 00-39, FCC 02-230 (rel. Aug. 9, 2002).

together: (1) a critical mass of compelling digital content; (2) distribution of that content to consumers; and (3) reception equipment in consumers' hands."⁶ The goal of this proceeding is to facilitate the first condition – ensuring that a critical mass of compelling digital content is available. Though, as explained below, there is reason to question the achievability of a market-based broadcast copy protection solution, Motorola believes that such a solution should be vigorously pursued prior to any regulatory action.

11. Realistic Acknowledgement of Security Challenges is Necessary to Ensure Appropriate Level of Investment in Digital Broadcast Copy Protection Solutions and to Facilitate the Transition to DTV.

An examination regarding the security of digital content involves a balancing of the costs of prevention of theft with the likelihood of theft and the damage that theft would cause to the injured party. Industry players are sometimes shortsighted with regard to investment in security at the introduction of new technologies since the industry strives to provide consumers with the lowest cost systems and products. For example, at the outset of the development of analog cable systems, most system operators did not understand the potential magnitude of piracy, and thus under-invested in security solutions. With their subsequent experience, these system operators invested heavily in conditional access systems for the digital cable upgrade. The National Cable Television Association Office of Signal Theft occasionally conducts studies on the level of signal piracy in North American cable networks, with recent estimates topping \$6.5 billion in annual losses.⁷ This amount is far in excess of the financial investment network

⁶ Separate Statement of Chairman Michael K. Powell, In *the Matter of Review of the Commissioner's Rules and Policies Affecting the Conversion to Digital Television*, MM Docket No. 00-39, FCC 02-230 (rel. Aug. 9, 2002).

⁷ See http://www.ncta.com/industry_overview/indOverView.cfm?indOverviewID=6.

operators have made in conditional access technology from Motorola and other vendors. Establishing effective security at the outset is a provably sound business practice.

In the DTV context, a relatively small number of technically savvy individuals could easily stimulate piracy. Given today's Internet-based communication environment, should a handful of people defeat any given copy protection, they would be able to distribute' pirated materials quickly to less technically savvy individuals.⁹ This type of communication-fuelled, widespread piracy, or even the threat of it, could cause content providers to withhold high value content from DTV distribution."

Government should be judicious in choosing to mandate any single digital broadcast copy protection approach. In this case, however, government action may be necessary to ensure a proper level of investment in effective security at the outset, to guarantee that high value content is available to DTV viewers, and to facilitate quick, ubiquitous deployment of a uniform DTV digital broadcast copy protection solution.

Motorola believes that the broadcast flag, as defined today without source encryption, is an ineffective security technology that will not ultimately serve the interests of the DTV transition or the consumer community

111. Any Comprehensive DTV Digital Broadcast Copy Protection Solution Must Encrypt at the Source.

Motorola experience with real-world piracy, as well as the experience of other companies, has demonstrated beyond a doubt the necessity of completely encrypting any

⁸ Conspicuous examples of this proliferation effect include the "DeCSS" breach of the DVD encryption scheme, the widespread use of Napster, and today's illicit peer-to-peer file sharing systems.

⁹ Experience has shown that problems can originate from as few as one creative individual, who then propagates his or her insights to a wide field of others. These others may not be creative enough to invent security breach technologies, but they faithfully pursue the potential profits derived therefrom

¹⁰ *See, e.g.*, Letter from Susan L. Fox, The Walt Disney Company, to Magalie Roman Salas, Secretary, FCC, CS Docket No. 97-80 (Nov. 8, 2001)

valuable material at the source. Given the magnitude of the potential piracy problem and the public interest benefits to be gained by facilitating the DTV transition, any ubiquitous solution must use security technology that is effective when viewed in light of similar past piracy problems and technological solutions.

Source encryption is overwhelmingly accepted as mandatory among the professional security technology community. High value content distributed over satellite and cable has been analog scrambled or digitally encrypted since the 1980's, and broadcast DTV should be no exception to this well-established, well-justified convention. Numerous examples of this encryption convention exist. All valuable satellite and cable TV content is encrypted, as are DVDs. Interfaces that traffic in digital TV content are fully encrypted, including the OpenCable POD Copy Protection System, 1394/5C Copy Protection, and DVI/HDMI High Definition Copy Protection (HDCP) standards. DOCSIS cable modem traffic is encrypted, as well as PacketCable cable telephony and most digital cellular networks. Even sensitive Internet browser traffic is encrypted using Secure Sockets Layer (SSL), Secure Hyper Text Transfer Protocol (SHTTP), or dedicated virtual private networks (VPNs). The use of source encryption is so well-established and commonplace that networks which traffic in valuable content without source encryption are the exception, not the rule. The lack of source encryption in broadcast DTV is extraordinarily conspicuous in this regard.

A number of existing copy protection standards (*e.g.*, OpenCable POD and 1394/5C) label content according to its value, so that it can be processed with the appropriate levels of security protection. These levels are “copy freely” for the lowest value content, “copy once” or “copy no more” for intermediate value content, and “copy

never” for high value content. An agreed convention arose in these standards, where the lowest value “copy freely” content was not to be source encrypted, while the other higher value grades were always source encrypted. This demonstrates the established convention that clear content is, by definition, content not intended for protection. These standards always completely encrypt any content that is protected, from its source transmission point to its “sink” reception point (e.g., a display device or DTV). Among the community of security professionals, protection of content is synonymous with source encryption.

The BPDG discussion group chose broadcast flag technology because its mandate was constrained; as the BPDG Final Report notes, a more efficient solution of encryption was suggested but was not considered by BPDG given the political and business climate.” Concern over potential financial responsibilities associated with encryption equipment upgrades are likely a major reason for this constraint, as is concern over disruption of early adopters of DTV who might need new decryption devices to continue operating. There may also be a mistaken belief that encrypting a DTV transmission is equivalent to making it a Pay TV service, which is not the case.

IV. Deployment of Source Encryption for DTV Need Not Disenfranchise Early Adopter Consumers

It is not necessary that currently-deployed DTVs be replaced or even augmented to facilitate broadcast copy protection that utilizes source encryption. As stated above, a convention has long existed where protection of content is synonymous with encryption

¹¹ Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group at 3, n. 3 (June 3, 2002) (“It was suggested that a more effectual technical and enforcement solution would be to encrypt DTV content at the source (*i.e.*, the transmitter). Given the current political **and** business environment, this approach was rejected by motion picture studios and broadcasters, **as well as** by representatives of consumer electronics manufacturers...”).

of content. But not all content owners demand that their material be protected (*i.e.*, encrypted). Some advertising revenue-based services seek the widest audience possible and are less concerned about the need to source encrypt, for example. However, premium or long-lived” content must be source-encrypted to protect it, as has been the well-established convention since Home Box Office was first encrypted in 1986. Source encryption is absolutely necessary to protect high-grade content effectively, but is not necessarily needed for lesser-valued or some advertising revenue-based material.

This multi-valued content situation allows us to deploy broadcast copy protection while minimizing the impact to the existing deployed base of early adopters. This is achieved by establishing a basic requirement on any broadcast protection technology – *i.e.*, that source encryption only be activated for premium or long-lived content, and that source encryption be turned off for other content whose owners do not require it. This ability to turn encryption on and off is fundamental to the several copy protection standards already mentioned, and is used to differentiate “copy freely” content from higher value grades. Even the existing MPEG standard contains this simple capability.

This source encryption enablement capability allows the existing early adopter consumer population to receive “copy freely” content for numerous years into the future, without any new equipment. The early adopter population would always have access to the unencrypted “copy freely” grade of content, but would not be able to receive the encrypted higher grades without obtaining new, source decryption-enabled devices.

¹² We use the common phrase “long lived” to denote classical or so-called “evergreen” content that maintains its value over many years. The Walt Disney Company owns the most widely-known examples of this, with content such as *Snow White* that holds its value for each succeeding generation of consumer.

V. Source Encryption Equipment Upgrades Are Optional, Not Mandatory, and Can Be Financed Through Normal Competitive Market Forces

Each individual early adopter consumer would be able to elect the purchase of new, broadcast copy protection decryption equipment or not, based purely on the desirability of the content such gear would allow them to access. This should be a market –based decision, where consumers have the choice, and the companies that offer DTV have the incentive to compete in satisfying the consumer through compelling offerings. Early adopter consumers who choose not to purchase any upgrade equipment will still have access to a variety of “copy freely”, non-premium, non-long-lived material.

To offer upgrade equipment to consumers who so desire, various technical solutions will have to be designed to support early adopter DTVs that have been deployed without source decryption technology, as well as the existing analog TV base. Families of devices will have to be developed that would act as bridge products to address analog televisions and the DTVs that have already been deployed without the encryption technology. But such devices will naturally arise when consumers perceive a range of content with different values, and make their choices through competitive service selection and equipment acquisition.

Typically, we would expect the open marketplace and its offerings to motivate those consumers interested in premium or long lived content. Where needed, however, funding of these bridge products could conceivably be subsidized where it makes business sense for a service operator. Such subsidy scenarios have developed in the satellite TV market, and are plausible in DTV. We should note that, while there is no mandate for such subsidies in DTV, neither is there any prohibition.

If the above scenario of mixed encrypted and unencrypted content is not acceptable for some reason, it is still possible to have a hard cut-over. The current DTV base is still relatively small, and will remain so for the next year or so, and thus the cost of even government-subsidized converters is simply not that high.

VI. Source Encryption Is Not Synonymous With Pay TV, and Can Be Applied to Free TV Where Needed for Copy Protection Security

Free TV can be encrypted – *i.e.*, encryption systems do not need to be Pay TV systems to operate and to protect content.¹³ In order for any source encryption broadcast copy protection solution to work, new DTVs will have to include the ability to decrypt. This is a digital function of smaller cost magnitude than other technologies that have been discussed in various contexts (*e.g.*, a mandated VSB demodulator). A free DTV broadcast copy protection system would use technologies very similar to today's Pay TV systems. There is no requirement that such effective security technologies only be applied to Pay TV applications.

VII. Any Mandated Source-Encrypting Digital Broadcast Copy Protection Solution Must Provide for a Minimal Licensing or Cost Burden

In order for any source-encryption DTV solution to be deployed widely, any licensing burden must be low to facilitate the most rapid and widest possible usage in DTVs and DTV compatible devices. Further, implementations of such technology for DTV digital broadcast copy protection must be provided at a minimized cost, so as not to adversely affect the equipment cost decreases that are paramount to wide DTV

¹³ Motorola and other digital content protection vendors have various customers who use our digital encryption products for non-fee-based services. Examples include private networks who require encrypted video communication to protect their private corporate transmissions, or so-called "backhaul" networks that move content around the globe, but only among corporate or other organizations outside the consumer marketplace. In various other standards – *e.g.*, DOCSIS or wireless encryption protocol (WEP) or SSL – encryption is used to protect digital data of various types from a variety of eavesdropping or other copy-protection-related purposes, with no fee payment required.

deployment. Motorola has deployed similar or equivalent standards-based security technology in large volume already, and is convinced that very cost effective implementations are realistic.

To maximize viability, any contract to use this technology must not include burdensome licensing terms that prevent the solution from being freely available and universally deployed. As is common in today's leading edge technology standards, such broadcast copy protection technology must be made openly available to all interested parties under fair, reasonable, and non-discriminatory terms.

VIII. Any Mandated Digital Broadcast Copy Protection Solution Must be Administered by a Transparent Process Governed by an Open Governing Body

The technology for source encryption of DTV must be developed through a standards-based process, be it an existing body or one that follows typical standards rules and processes and is convened exclusively for DTV broadcast copy protection. Such a technology standard must be completely open, without closed-door meetings or private decision making processes.

However, a separate governing body should be established to handle various broadcast copy protection implementation, deployment, and usage issues including licensing the numerous manufacturers who will need the technology for DTVs and related products. This body will also need to address a number of related issues over the long term, including evolution of the security technology in event of breach, and contingency plans for revocation of rogue devices or encryption technology from parties who have misused information or technology. This body must exist separate and apart from any technology standards organization and have as its charter implementation issues such as the "robustness rules" and processes to ensure proper use of the technology.

The governing body must have a balanced membership that includes representatives from all stakeholders. The governing body must be managed by a transparent process that is auditable and open.

While such a body may not necessarily be formally convened by the FCC as a Federal Advisory Committee and may exist as an industry and market led initiative, the rules established in the Federal Advisory Committee Act¹⁴ may serve as a model:

- (i) Charter” establishing the scope of work and responsibility of the committee drafted and published;
- (ii) require the membership of the committee to be fairly balanced in terms of the points of view represented;
- (iii) Notice of meetings published in Federal Register; and
- (iv) Detailed minutes of the meeting kept, including a record of the persons present.¹⁶

By following this type of open process, all affected stakeholders will be able to participate in a meaningful way in the initial technology standardization, as well as the governance and control of the copy protection system. In this way, one entity or group will not be able to dominate the management of the system or its technology.

¹⁴ 5 U.S.C., App. 2 (1988).

¹⁵ The charter establishing the governance body must detail the rules for voting, due process rights and appeals processes.

¹⁶ Federal Advisory Committee Act, 5 U.S.C., App. 2 (1988).

CONCLUSION

The issues surrounding the transition to digital television, including the issue of how to protect high value content in a mass media broadcast environment, are complex but manageable. Motorola looks forward to working with other industry leaders and the Commission to find solutions to better enable the transition.

Respectfully Submitted,

_____/s/_____

Jeanine Poltronieri

Director

Telecommunications Strategy and Regulation

_____/s/_____

Eric J. Sprunk

Senior Director, Advanced Technology

Broadband Communications Sector

Motorola

1350 I Street, NW

Washington, DC 20005-3305

Tel: 202-371-6870

Dated: December 6, 2002